REMARKS

Introduction

This Reply is in response to the Office Action of November 5, 2010. Reconsideration of this application in view of the following remarks is respectfully requested.

Subject Matter Indicated to be Allowable

Claims 1-12, 18, and 19 were allowed. Applicants hereby reserve the right to pursue the subject matter of these claims during subsequent prosecution should the present Reply not be considered to place this application in condition for allowance.

Claim Objections

Claims 14 and 15 were objected to for minor informalities. Claims 14 and 15 have been amended as requested in the Office Action. Applicants respectfully request the claim objections be withdrawn.

The Prior Art Rejections

In the Office Action, claims 13-17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gentry et al. U.S. Patent No. 7,353,395 in view of Deng et al. U.S. Patent No. 6,910,129. These rejections are respectfully traversed.

Claims 13-17

As explained by applicants in the August 31, 2010 Reply, nothing like the arrangement of claim 13 is shown or suggested by Gentry and Deng.

As background, applicants note that the rejection suggests that Gentry's public key P_A is the claimed commitment, Gentry's shared secret S_{AB} is the claimed secret value, and Gentry's private key S_A is the claimed decommitment.

The "Response to Arguments" relied upon a statement that "Gentry further discloses using the IBE private key to compute a public key (i.e., commitment) and private key (i.e., decommitment) (Gentry: column 5 lines 10-12: PKG determines the first entity's private key Sa...provide private key to the first entity and column 6 lines 64-66: generator g is used to create public keys Pa, Pb)." This statement is erroneous for multiple reasons.

Firstly, Gentry does not use an IBE private key to compute a public key. In fact, the opposite is true. Gentry computes private keys from public keys. In particular, Gentry applies a hash function to a user's identity to create the user's public key P_A. Gentry's private key generator then determines the user's private key S_A from a master secret s and the user's public key P_A (e.g., Gentry computes $S_A = sP_A$) (see,

e.g., col. 5, lines 6-12 of Gentry).

Secondly, Gentry does not disclose using an IBE private key to compute a private key. The circular nature of the rejection's suggestion makes its logical fallacy clear. (Applicants note that the "private key" referred to in this section of the "Response to Arguments" section must be Gentry's private key S_A, which was suggested be equivalent to the claimed decommitment, rather than Gentry's shared secret S_{AB}, which was suggested to be equivalent to the claimed secret value. The rejection confirms this fact with the "(i.e., decommitment)" portion of the statement.)

Thirdly, Gentry's public and private keys are not commitments and decommitments (see the additional argument below).

The "Response to Arguments" also relied upon a statement that "Deng does disclose using a symmetric key that is based on an IBE private key to encrypt a commitment or a decommitment." The rejection noted that "the key K cited in the above column can either be a public key (i.e., commitment) or a private key (i.e., decommitment)." The rejection's statements are incorrect and based on a misunderstanding of the differences between commitment schemes and public and private keys. Public keys are not a commitment to a secret value. Private keys are not a decommitment.

Commitment schemes allow a first user to commit to a secret value, while maintaining the secrecy of the secret value, by computing a commitment. The commitment is provided to a second user (at time t_1). At a later time (time t_2), the first user provides the second user with a decommitment that allows the second user to verify or retrieve the secret value. Because the second user had the commitment in hand at time t_1, the second user is assured that the first user could not have changed the secret value between times t_1 and t_2.

For at least additional reasons, claim 13 is patentable over Gentry and Deng even if these references are combined. Claims 14-17 depend from claim 13 and are allowable at least because claim 13 is allowable.

Conclusion

The foregoing demonstrates that claims 1-19 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

The Commissioner is hereby authorized to charge any

fees due in connection with this submission to Deposit Account No. 502942.

Respectfully submitted,

Date: February 8, 2011

/David C. Kellogg/
David C. Kellogg
Reg. No. 62,958
Telephone: 415-837-0659
Agent for Applicant
Customer No. 36532